
PACK DE CONFORMITÉ
ASSURANCE
CNIL
Commission Nationale de l'Informatique et des Libertés
Édition juillet 2014
cnil.fr

SOMMAIRE







PACK DE CONFORMITÉ

ASSURANCE

LA DÉMARCHE

Le pack de conformité est un nouvel outil de régulation de l'utilisation des données personnelles qui recouvre tout à la fois :

- ***une méthode de travail :*** *il s'agit pour la Cnil d'associer pleinement les acteurs d'un secteur d'activité (professionnels à titre principal mais aussi, le cas échéant, les autorités publiques et usagers concernés) afin de faire remonter les bonnes ou mauvaises pratiques, les problèmes rencontrés, les demandes des usagers, les spécificités du secteur concerné et plus généralement les questions qui se posent sur le terrain.*

- ***un nouveau mode de régulation pour la Cnil :*** *Il s'agit de bâtir des référentiels sectoriels, mettant à plat les traitements de données personnelles du secteur pour déboucher sur :*
  - *un ensemble de règles et de bonnes pratiques déclinées au moyen des vecteurs juridiques existants tels que normes simplifiées, autorisations uniques, recommandations, reconnaissance de la conformité des règles professionnelles, mais aussi des fiches pratiques élaborées pour clarifier et donner des exemples concrets.*
  - *des modes opératoires et processus organisationnels liés à la mise en place de correspondants informatique et libertés, de règles internes d'entreprises (appelés BCR), de labels…*

Ce référentiel a un double objectif :

- *sécuriser juridiquement les professionnels en donnant des indications concrètes sur la façon de respecter les textes et des modes opératoires précis.*
- *simplifier les formalités autant que la loi actuelle le permet, en utilisant les dispenses, normes simplifiées et autorisations uniques.*

LE SECTEUR DE L'ASSURANCE

Depuis quelques années, on assiste à une montée en puissance du secteur de l'assurance dans une société où le vieillissement des populations, la mondialisation des économies ou encore le droit européen de l'assurance connaissent d'importantes mutations. Ces dernières ont pour conséquences directes une course à la compétitivité et une multiplication des produits. Dans ce contexte de transformation du marché, les assureurs recherchent de plus en plus une offre de services globale pour mettre sur pied des applications immédiates, au service de leur stratégie et de leurs performances.

Pour faire face à la demande de nouveaux produits, de nouveaux modes de distribution, et des évolutions législatives, la Cnil et les professionnels de l'assurance ont souhaité se réunir pour examiner l'ensemble des traitements nécessitant la collecte de données personnelles. La Cnil a ainsi souhaité accompagner les professionnels de l'assurance - représentés par les organisations professionnelles, FFSA, GEMA, FNMF, CTIP et CSCA - dans la démarche de simplification des formalités et de sécurisation juridique en donnant des indications concrètes sur la façon de respecter la loi informatique et libertés et en proposant des modes opératoires détaillés.

Le groupe de travail constitué pour le « pack assurance »

La Cnil a convié l'ensemble des acteurs de la place du secteur de l'assurance à participer aux travaux nécessaires pour mener ensemble l'élaboration du pack de conformité. Des ré- »»







unions trimestrielles ont été organisées avec les organisations professionnelles du secteur (FFSA, GEMA, FNMF, CTIP et CSCA). De leur côté, les organisations ont également réuni leurs membres pour organiser des réunions de travail et procéder aux relectures des textes et participer de façon effective à la construction du pack.

Groupe de travail	Membres	Missions et principes directeurs
FFSA / Fédération Française des Sociétés d'Assurances	234 entreprises[1]	Représenter les intérêts de la profession auprès de ses interlocuteurs, publics et privés, nationaux et internationaux. Être un outil de concertation avec ses différents partenaires tant externes[2] qu'internes[3]. Étudier en commun les problèmes techniques, financiers et juridiques. La FFSA établit des statistiques rétrospectives et prospectives de l'assurance. Informer le public.
GEMA / Groupement des entreprises Mutuelles d'Assurance	45 sociétés adhérentes	Le GEMA est le syndicat professionnel des mutuelles d'assurance. Il défend une vision mutualiste des questions d'assurance auprès des pouvoirs publics nationaux et européens et des organismes professionnels. Les mutuelles d'assurance constituent une famille à part entière qui se distingue des autres sociétés d'assurance par certaines caractéristiques essentielles : - Les mutuelles d'assurance sont des sociétés de personnes qui n'ont pas de capital social, donc pas d'actionnaires à rémunérer - Les sociétaires, entre eux, sont à la fois assurés et assureurs - Les mutuelles d'assurance sont à but non lucratif - Les mutuelles d'assurance sont gérées par des administrateurs bénévoles élus par des délégués eux-mêmes élus par les sociétaires. Les valeurs fondatrices de solidarité, de démocratie, de liberté et de transparence sur lesquelles s'appuient les mutuelles d'assurance sont les garants de leur indépendance, du maintien du lien direct avec leurs sociétaires et du contrôle du fonctionnement et de la gestion.
FNMF / Mutualité Française	95 % des mutuelles 38 M personnes	La mission d'une mutuelle est simple : garantir à tous l'accès à des soins de qualité. - Limiter les dépassements d'honoraires. - Généraliser le tiers payant. - Maintenir une action sociale. - Solidarité, démocratie et transparence. - Les mutuelles font vivre un système de solidarité, d'entraide et de prévoyance. Il permet l'accès à des soins de qualité à tous les adhérents. - Les mutuelles combattent l'exclusion et la discrimination. Elles ne sélectionnent pas leurs adhérents.
CTIP / Centre technique des institutions de prévoyance (IP)	47 IP 13 M salariés 2 M entreprises	Représenter les IP auprès des pouvoirs publics nationaux et européens. Favoriser le développement des IP en préservant leur vocation sociale et la spécificité de leur gestion paritaire.

(1) Soit 90 % du marché français de l'assurance et près de 100 % de l'activité internationale des entreprises de ce marché.
(2)consommateurs, médias, universitaires, autres secteurs d'activité…
(3) organisations d'intermédiaires, syndicats de salariés (négociations des conventions et accords collectifs)







CSCA / Chambre Syndicale des Courtiers d'Assurances	Plus de 1 000 adhérents[4]	Porter la représentativité des syndicats adhérents auprès des pouvoirs publics, des organisations patronales, salariales, professionnelles
		Défendre et promouvoir les intérêts moraux et matériels des syndicats adhérents et de leurs membres
		Veiller au respect par ses membres des règles déontologiques, professionnelles et de solvabilité
		Étudier les questions professionnelles, économiques, juridiques et sociales, relatives à l'activité de courtage d'assurances et/ou de réassurances
		Représenter en justice la profession de courtier d'assurances et de réassurances, et assurer la défense et la protection des intérêts de la profession, etc.

Organismes communs : FFSA/GEMA : AGIRA (partenaire CTIP), l'AFLA, ARGOS,...

Le pack de conformité élaboré est un référentiel qui s'adresse aux responsables de traitements ayant la qualité « d'organismes d'assurance ». Cette notion regroupe les entreprises d'assurance (sociétés anonymes d'assurance, les sociétés d'assurance mutuelle, les mutuelles relevant du Code de la mutualité et les institutions de prévoyance), de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance (les agents généraux d'assurance, et les courtiers d'assurance).

Dans le cadre des autorisations uniques relatives au numéro de sécurité sociale « NIR » (AU n°31) et aux données d'infractions, de condamnations et mesures de sûretés (AU n°32), l'AGIRA[5] est également responsable de traitement.

- Pour l'AU n°31 cela s'explique par la reprise de l'AU n°18 dans son périmètre. En effet, le responsable de traitement visé par l'autorisation relative aux assurés et bénéficiaires de contrats d'assurance sur la vie décédés, est l'AGIRA.
- S'agissant de l'AU n°32, l'AGIRA est responsable de traitement au titre de son activité « TransPV »[6].

Le déroulement des travaux

1. Adoption de deux normes simplifiées

La Cnil dispose d'un pouvoir réglementaire qui lui permet d'édicter des normes destinées à simplifier l'obligation de déclaration pour les catégories les plus courantes de traitements. L'année 2013 a été l'occasion de mettre à jour la norme simplifiée n°16 relative à la passation, à la gestion et à l'exécution des contrats d'assurance et d'adopter une norme simplifiée n°56 pour la gestion commerciale des clients et prospects. Désormais, les organismes d'assurance pourront procéder à un engagement de conformité auprès de la Cnil pour les traitements concernant la gestion des contrats d'assurance, la gestion commerciale des clients, les opérations de prospection, ou encore l'élaboration de statistiques commerciales, etc.

Lien sur les délibérations

2. Adoption de trois autorisations uniques

Comme pour les normes simplifiées, la Cnil peut autoriser par une décision unique une catégorie de traitements répondant aux mêmes

(4) En 2010.
(5) Association pour la Gestion des Informations sur le Risque en Assurance.
(6) L'AGIRA fait partie de la liste des organismes que le procureur de la République peut autoriser à se faire délivrer une copie des pièces de procédure judiciaire en cours.







finalités, portant sur des catégories de données identiques et ayant les mêmes catégories de destinataires. Trois autorisations uniques ont été adoptées en 2014[7] : l'AU n°31 pour la collecte des données comportant le numéro de sécurité sociale « NIR », l'AU n°32 relative aux données d'infractions, de condamnations et mesures de sûretés et l'AU n°39 relative à la lutte contre la fraude en assurance[8].

- L'autorisation unique relative au « NIR » vise deux finalités : la collecte et le traitement du numéro de sécurité social et l'accès au répertoire national d'identification des personnes physiques (RNIPP) tel qu'il était prévu dans le cadre de l'AU n°18.
- Quant aux données d'infractions, de condamnations ou mesures de sûreté, elles peuvent s'avérer nécessaires lors de la passation, de la gestion et de l'exécution des contrats d'assurance. En effet, les données relatives aux infractions et condamnations font partie des antécédents du contrat d'assurance de l'assuré et permettent notamment à l'assureur d'évaluer les risques. De même, lors de l'exécution du contrat les données d'infractions peuvent être utilisées pour prouver que les conditions de garantie sont remplies et que le risque n'a pas été aggravé.
- Enfin, le périmètre retenu dans le cadre de la lutte contre la fraude est très large puisqu'il concerne la fraude interne et externe en matière d'assurance dommage et de personnes. Sont visés, toutes les phases de gestion de la fraude (prévention, détection et gestion des cas suspectés et avérés) pour les organismes d'assurances identifiés dans la norme simplifiée n°16 et dans le cadre de la passation, la gestion et l'exécution du contrat d'assurance.

Lien sur les délibérations

3. Adoption de fiches pratiques

Afin de faciliter la lecture de ces normes et ne pas alourdir le contenu des délibérations des fiches pratiques explicatives ont été rédigées. Elles ont vocation à aider les assureurs à mettre en œuvre concrètement les dispositions des normes et autorisations mais aussi à permettre aux assurés de mieux comprendre certaines notions techniques.

Lien sur les fiches pratiques
NS 56, NS 16, AU 31, AU 32, AU 39

RAPPEL

La Loi Informatique et Libertés

La loi informatique et libertés du 6 janvier 1978 modifiée s'applique dès lors qu'il est procédé à un traitement de données à caractère personnel :

- *Constitue un traitement de données personnelles toute opération (collecte, enregistrement, conservation, modification, extraction, consultation, utilisation, communication, interconnexion, destruction…) portant sur des données personnelles.*
- *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. Ainsi, sont des données personnelles toutes les données qui, seules ou combinées entre elles, peuvent être rattachées à un assuré, un client ou prospect (numéro de carte bancaire, références bancaires, vie maritale, nombre de personnes composant le foyer numéro d'acte de décès, données relatives aux investigations…). Les données personnelles ne sont donc pas uniquement les données nominatives (nom et prénom).*

La mise en place d'un traitement de données personnelles doit respecter la loi informatique et libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales (information des personnes quant au traitement mis en place, voire recueil du consentement, mise en place de modalités d'exercice du droit d'accès et de suppression des données, mesures de sécurité, formalités préalables à effectuer auprès de la CNIL…).

(7) Le 23 janvier 2014
(8) Le 17 juillet 2014



LEXIQUE

- **Adhérent :** Personne qui adhère, de manière obligatoire ou facultative au contrat collectif d'assurance souscrit par une personne morale au profit des membres.

- **Assuré :** Désigne une personne dont la vie, les actes ou les biens sont garantis par un contrat d'assurance :
  - Dans le domaine de l'assurance automobile, l'assuré est le propriétaire du véhicule. L'assuré est aussi « toute personne » qui, avec l'autorisation dudit propriétaire, possède la garde ou conduit du véhicule.
  - En matière d'assurances de bien, l'assuré est le preneur d'assureur mais aussi son conjoint, ses enfants mineurs et/ou majeurs célibataires qui vivent sous le même toit à l'adresse figurant sur le contrat d'assurance. Certains assureurs admettent aussi que toute autre personne résidant en permanence sous le même toit à l'adresse indiquée sur les conditions particulières, peut également être considérée comme assuré.
  - En assurances de personne, l'assuré est généralement le souscripteur du contrat sur lequel repose le risque (décès, maladie, invalidité).

- **Ayant droit :** Personne qui détient un droit en raison de sa situation juridique, fiscale, financière ou d'un lien familial avec le bénéficiaire direct de ce droit.

- **Bénéficiaire :** Tierce personne physique ou morale au profit de laquelle une assurance a été contractée. Elle peut être nommément désignée aux conditions particulières du contrat ou bien apparaître dans les conditions générales sous les termes de conjoint survivant, d'ayant droit ou d'héritier né ou à naître. Le bénéficiaire recevra l'indemnité due par l'assureur en cas de réalisation du risque assuré.

- **Le souscripteur :** Personne qui conclut, signe et règle les cotisations ou primes d'assurance. Il peut être différent de l'assuré ou du bénéficiaire. Le souscripteur peut être une personne physique (contrat individuel) ou une personne morale (contrat collectif).

- **Tiers victime :** Le tiers est généralement défini comme une personne n'ayant pas la qualité d'assuré et n'étant pas exclu du bénéfice du contrat. Cette notion est utilisée dans le cadre des contrats d'assurances de responsabilité civile. L'objet du contrat d'assurance de responsabilité civile est de garantir les conséquences pécuniaires de la responsabilité civile pouvant incomber à l'assuré en cas de dommages causés au tiers.



TEXTES APPLICABLES

- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés
- Code des assurances, code civil, code général des impôts, code monétaire et financier, code de la mutualité, code pénal, code des postes et des communications électroniques, code rural, code de la santé publique, code de la sécurité sociale, code du travail, code de la consommation.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
- Ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques.



FICHE N°1 LA PASSATION, LA GESTION ET L'EXECUTION DES CONTRATS D'ASSURANCE (NS 16)

LES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS

La mise en place d'un traitement de données personnelles doit respecter la loi I&L. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

Finalités poursuivies par le traitement

● **Finalité 1 : passation et la gestion des contrats[1] :**

- **La passation des contrats :** Il s'agit de « l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés » notamment dans le cadre du respect de l'obligation de conseil (art. L.520.1 et L.132-27-1 du Code des assurances). Cette obligation nécessite de préciser les exigences et besoins du souscripteur éventuel, et les raisons justifiant le conseil donné pour un produit d'assurance déterminé.
  Cela concerne aussi « l'examen, l'acceptation, le contrôle et la surveillance du risque ». On parle couramment de « l'appréciation des risques ». Elle comprend l'examen et l'évaluation des caractéristiques du risque pour en déterminer en particulier la fréquence, son coût moyen, le coût du sinistre maximum possible, afin d'établir une tarification et de vérifier l'assurabilité du risque[2].
- **La gestion des contrats :** La gestion des contrats couvre la phase pré contractuelle jusqu'à la résiliation du contrat. Il s'agit notamment de la tarification, de l'émission des documents pré contractuels, contractuels et comptables, de l'encaissement des primes ou cotisations, de leur répartition éventuelle entre les coassureurs et les réassureurs, du commissionnement, de la surveillance des risques, et des autres opérations techniques nécessaires.

Aucune décision refusant un contrat à une personne ne pourra avoir pour seul fondement un traitement automatisé de données à caractère personnel, les personnes concernées devront être mises en mesure de présenter leurs observations.

● **Finalité 2 : l'exécution des contrats[3] :** Il s'agit des opérations techniques nécessaires à la mise en œuvre des garanties et des prestations. Dans ce cadre, les données collectées sont relatives à la gestion des prestations, à la gestion des sinistres. Dans certains cas, il est possible que l'apériteur[4] procède à la collecte de ces informations auprès des coassureurs et des réassureurs au moment de la souscription du contrat d'assurance ou lors de l'exécution des dispositions contractuelles.

● **Finalité 3 : l'élaboration des statistiques et études actuarielles.**

● **Finalité 4 : l'exercice des recours et la gestion des réclamations et des contentieux.**

● **Finalité 5 : l'exécution des dispositions légales, réglementaires et administratives en vigueur à l'exception de celles qui relèvent d'une formalité particulière prévue par la loi I&L :** Il peut s'agir de traitements relatifs à l'exécution des règles fiscales, sociales, ou encore à la collecte de contributions pour différents fonds (ex : fonds de garantie des assurances obligatoires, fonds de prévention des risques naturels majeurs).

Les dispositions qui relèvent d'un régime particulier sont par exemple, celles dont les données sont soumises à un régime d'auto- »»

(1) Le terme contrat fait référence aux contrats d'assurance, de capitalisation, de réassurance, et d'assistance.
(2) L'assureur a l'obligation de respecter des règles prudentielles qui le conduisent à définir une politique d'acceptation des risques et refuser les risques qu'il ne peut assurer selon cette politique (article R.336-1-2° du code des assurances et article 41 de la directive 2009/138).
(3) Le terme contrat fait référence aux contrats d'assurance, de capitalisation, de réassurance, et d'assistance.
(4) En matière d'assurance couverte par plusieurs assureurs, celui d'entre eux qui, d'une manière générale, représente le groupe d'assureurs.









FICHE N°1

LA PASSATION, LA GESTION ET L'EXECUTION DES CONTRATS D'ASSURANCE (NS 16)

risation (ex : NIR, données d'infraction…) ou encore, celles relevant de la réglementation spécifique à un secteur (ex : lutte anti-blanchiment…).

Catégories de données

Une fois les personnes informées de la mise en œuvre du traitement, les données qui les concernent doivent être pertinentes et proportionnées au regard de la finalité.

- **Les données relatives à l'identification :** Il s'agit « des données relatives à l'identification des personnes parties, intéressées ou intervenantes au contrat : état civil ainsi que les pièces justifiant l'identité, les coordonnées et la nationalité ».
  - **Les personnes parties et intéressées au contrat** sont notamment les assurés, les bénéficiaires, les ayants droits, les tiers, les témoins, les souscripteurs, les héritiers, les tuteurs, les curateurs, les payeurs de prime, les conducteurs, les cautions…
  - **Les personnes intervenantes au contrat** sont notamment les intermédiaires en assurance, les gestionnaires, les prestataires (ex : les réparateurs automobiles, les agents de recherche privé, les experts, les avocats, les médecins, les enquêteurs, les professionnels de santé, les réseaux de soins, les officiers ministériels : notaires, huissiers…).

Les documents d'identification pouvant être collectés sont relatifs à :

- **L'état civil :** il s'agit notamment des noms, prénoms, sexe, civilité, données relatives aux pièces d'identité (permis de conduire, carte identité, livret de famille, carte de séjour, passeport…), date de décès, nom jeune fille, date et lieu de naissance…
- **Aux coordonnées :** il s'agit notamment des adresses, numéros de téléphone (fixe et mobile), numéro de télécopie et adresses électroniques, code interne de traitement permettant l'identification du client…
- **À la nationalité :** connaître la nationalité exacte des personnes parties ou intéressées au contrat permet à l'assureur de savoir : s'il peut proposer un contrat d'assurance à une personne ne résidant pas dans l'Union Européenne, ou la législation applicable au contrat d'assurance si cette personne réside dans l'UE[5]. La nationalité est l'une des informations qui permet de déterminer quelles sont les éventuelles obligations (ex : fiscales à l'égard de l'État dont le souscripteur est un ressortissant).



ATTENTION

Conclure un contrat d'assurance avec une personne étrangère a pour conséquence le respect de la législation de son pays notamment en matière fiscale (réglementation FATCA ou convention fiscale applicable).

- **Les données relatives à la situation familiale, économique, patrimoniale et financière :** Il s'agit « des données relatives à la situation familiale, économique, patrimoniale et financière » des personnes parties ou intéressées au contrat et nécessaires à son application.
  - **Les données relatives à la situation économique et financière sont les éléments relatifs aux :** revenus du travail et autres revenus, aux valeurs mobilières, au patrimoine immobilier, aux encours et à l'endettement, aux titres détenus, aux relevés de comptes titres, aux données d'imposition, aux crédits, aux revenus imposables, au numéro de chèque, au numéro de carte bancaire, à la date de fin de validité de la carte bancaire, aux frais généraux, au capital souscrit/remboursé, aux références bancaires (RIB, IBAN, BIC, relevé postal) à la situation de surendettement ou d'ouvrant droit à avantages assurantiels - bénéficiaires CMU, RSA…
  - **La situation patrimoniale :** concerne les biens du patrimoine (notamment les biens immobiliers).
  - **La situation familiale :** concerne la situation matrimoniale (mariage, pacs, concu-

(5) Règlement n°593/2008 du 17 juin 2008 relatif à la loi applicable aux obligations contractuelles -Rome I



FICHE N°1
LA PASSATION, LA GESTION ET L'EXECUTION DES CONTRATS D'ASSURANCE (NS 16)

binage…), la composition du foyer, le nombre de personnes composant le foyer, le nombre et l'âge du ou des enfant(s)…

- **Les données relatives à la situation professionnelle :** Il s'agit « des données relatives à la situation professionnelle » des personnes parties ou intéressées au contrat (souscripteurs, assurés, adhérents…) et nécessaires à son application.

Sont concernés : la catégorie socioprofessionnelle, le domaine d'activité, la profession et selon les catégories de contrat : l'employeur, les catégories de personnels assurés, la branche, la convention collective, le n° SIRET / SIREN, la raison sociale, les revenus ou le chiffre d'affaires, la date prévisionnelle de départ à la retraite, le régime fiscal, les compétences et qualifications professionnelles, les justificatifs de demandeur d'emploi…

- **Les données nécessaires à l'appréciation du risque :** la situation géographique, les caractéristiques du logement ou du local, les conditions d'occupation, les renseignements sur les biens assurables, le type et les caractéristiques du ou des biens assurés, les informations relatives à la sinistralité et les antécédents, le permis de conduire et sa validité, et le cas échéant si le bien est utilisé sur le lieu de travail et lors de déplacements professionnels, éléments entraînant une déchéance de garantie…

- **Les données nécessaires à la passation, l'application du contrat et à la gestion des sinistres et des prestations :** Il s'agit des données :
  - **liées au contrat :** le numéro d'identification du client, de l'assuré, du contrat, du dossier sinistre, le mode de paiement, les primes, les cotisations et accessoires, les commissions, les taxes, les créances en cours, les références de l'apporteur, des coassureurs et des réassureurs, la durée, les garanties, les montants, les exclusions, l'autorisation de prélèvement, les données relatives aux moyens de paiement ou relatives aux transactions telles que le numéro de la transaction, le détail de l'opération relative au produit ou service souscrit, les impayés, le recouvrement…
  - **liées au sinistre :** la nature du sinistre, les indemnités, la valeur assurée et les garanties souscrites, la description des atteintes aux biens, les rapports d'expertise, les rapports d'enquête…
  - **liées à la victime :** le taux invalidité/incapacité, les rentes, le capital décès, les montants des prestations, la fiscalité, les modalités de règlement, la réversion, les indemnités chômage, les montants remboursés par la sécurité sociale pour les complémentaires frais de soins (maladie, maternité…)…

- **Les informations relatives à la détermination ou à l'évaluation des préjudices.**

- **Les données relatives à la localisation des personnes ou des biens :** Ces données sont des informations essentielles dans le cadre des garanties d'assistance et d'assurance (recherches des véhicules perdus ou volés, éco-conduite, assistance aux personnes malades ou en difficultés…).

- **Les données relatives à la vie personnelle et aux habitudes de vie :** Il s'agit « des données relatives à la situation personnelle et aux habitudes de vie en relation avec les risques assurés » et nécessaires à l'application du contrat.
  - **Les données relatives à la situation personnelle** sont la situation de famille, le régime juridique particulier applicable à la situation de famille, le nombre d'enfants, les descendants, les ascendants et personnes à charge, les études et la formation, la capacité et le régime de protection (minorité, tutelle, curatelle) et invalidité…
  - **Les données relatives aux habitudes de vie** sont les loisirs, activités sportives et de plein air, la pratique de la chasse, de la plaisance, les trajets, les kilométrages parcourus…

- **Les données relatives à la santé :** Au moment de la conclusion d'un contrat il faut obtenir l'accord de l'intéressé pour le recueil de ses données de santé. C'est aussi le cas au moment de la gestion du sinistre sauf impossibilité (ex : personne en incapacité physique ou intellectuelle de consentir du fait de ses préjudices corporels).

Cette obligation n'existe pas non plus en matière de gestion des sinistres automobile, puisque l'assureur a une obligation légale de recueillir des données médicales[6] (descriptions









FICHE N°1

LA PASSATION, LA GESTION ET L'EXECUTION DES CONTRATS D'ASSURANCE (NS 16)

des atteintes, copies des certificats médicaux et autres pièces justificatives, numéro de sécurité sociale) pour proposer une indemnisation aux victimes.

Dans certains cas et lorsque la sauvegarde de la vie de la personne et l'urgence des situations prévalent, il n'est pas toujours possible de recueillir le consentement de la victime au moment de sa prise en charge.

Durées de conservation

- **Des données lors de la conclusion d'un contrat :** Les durées de conservation doivent permettre de respecter les délais de prescriptions qui résultent, notamment, du code des assurances[7] et du code civil[8]. En outre, l'assureur a une obligation[9] de conserver les données du relevé d'information détaillant les antécédents d'une personne en tant qu'assurée auto ou moto au cours des 5 dernières années.
- **Des données en l'absence de conclusion d'un contrat :** Les données peuvent être conservées pendant un délai de 3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (demande de renseignements ou de documentation, par exemple).
- **Des données relatives à la carte bancaire :**
  - Ces données doivent être supprimées lorsque la transaction est réalisée soit au moment de son paiement effectif. Dans le cas d'un paiement par carte bancaire, elles peuvent être conservées pour une **finalité de preuve pendant 13 mois** suivant la date de débit[10] en cas d'éventuelle contestation de la transaction. Ce délai peut être étendu à 15 mois pour tenir compte des cartes de paiement à débit différé.
  - Enfin, il est possible de **conserver plus longtemps les données de la CB avec le consentement exprès du client** (ex : case à cocher. En revanche cet accord ne peut pas résulter de l'acceptation de conditions générales).
  - Les données du **cryptogramme visuel** ne doivent pas être stockées.
  - Lorsque la date d'**expiration de la carte bancaire est atteinte**, les données relatives à celles-ci doivent être supprimées.
- **Des données de santé :**
  - **Si le contrat n'a pas été conclu :** le responsable de traitement peut conserver les données de santé pendant une durée maximale de 5 ans[11] (2 années en archivage courant et 3 ans en archivage intermédiaire). Cette durée se justifie par le fait que le responsable de traitement doit pouvoir répondre aux demandes formulées par un assuré pour des décisions de révision de son contrat ou à des demandes de médiation.

Destinataires

Les destinataires ayant accès aux données à caractère personnel sont les personnes habilitées et agissant dans le cadre de leurs attributions.

- **Dans le cadre des missions habituelles :**
  - les personnels chargés de la passation, la gestion et l'exécution des contrats,
  - les délégataires de gestion, les intermédiaires d'assurance, les partenaires,
  - les prestataires,
  - les sous traitants, ou les entités du groupe d'assurance auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions,
  - s'il y a lieu les organismes d'assurance des personnes impliquées ou offrant des prestations complémentaires,
  - s'il y a lieu les coassureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties,
  - les personnes intervenant au contrat tels que les avocats, experts, auxiliaires de justice et officiers ministériels, curateurs, tuteurs, enquêteurs et professionnels de santé, médecins-conseils et le personnel habilité,
  - Les organismes sociaux lorsque les régimes sociaux interviennent dans le règle-

(6) Article R.211-37 du code des assurances.
(7) Articles L 114-1 et L 114-2 du code des assurances.
(8) Les articles 2224 à 2227.
(9) Article A.121-1 et 12 du code des assurances.
(10) Article L. 133-24 du code monétaire et financier.
(11) C'est aussi le délai de prescription des actions civiles (article 2224 du code civil).









FICHE N°1
LA PASSATION, LA GESTION ET L'EXECUTION DES CONTRATS D'ASSURANCE (NS 16)

ment des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux.

- **En qualité de personnes intéressées au contrat :**
  - Les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats et s'il y a lieu, leurs ayants droit et représentants,
  - S'il y a lieu les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat,
  - S'il y a lieu le responsable, les victimes et leurs mandataires ; les témoins, les tiers intéressés à l'exécution du contrat.
- **En qualité de personnes habilitées au titre des tiers autorisés :**
  - S'il y a lieu les juridictions concernées, les arbitres, les médiateurs,
  - Les ministères concernés, autorités de tutelle et de contrôle et tous organismes publics habilités à les recevoir,
  - Les services chargés du contrôle tels que les commissaires aux comptes et les auditeurs ainsi que les services chargés du contrôle interne.

Information et droits des personnes

- **La personne doit être informée, préalablement à la mise en œuvre du traitement :** de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.
- **À ce titre, elle dispose d'un droit d'accès, de rectification et d'opposition.**
- **L'information des personnes sur le site internet :** Les données de connexion (date, heure, adresse Internet, protocole de l'ordinateur du visiteur, page consultée) pourront être exploitées à des fins de mesure d'audience et d'assistance technique. Dans ce cas, le consentement préalable des personnes n'est pas nécessaire, à condition qu'ils disposent d'une information claire et complète délivrée par l'éditeur du site internet, d'un droit d'opposition, d'un droit d'accès aux données collectées et qu'elles ne soient pas recoupées avec d'autres traitements tels que les fichiers clients.
  - Cette information peut, par exemple, figurer dans les courriers électroniques, sur la page d'accueil du site ou dans les conditions générales d'utilisation.
  - Le droit d'opposition à l'analyse de sa navigation : l'outil permettant de désactiver la traçabilité mise en œuvre par l'outil d'analyse de fréquentation doit remplir les conditions suivantes :
    - Un accès et une installation aisés pour tous les internautes sur l'ensemble des terminaux, des systèmes d'exploitation et des navigateurs internet ;
    - Aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.
  - Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a déjà été au préalable, de la finalité de toute action tendant à accéder à des informations déjà stockées dans son équipement terminal de communications électroniques ou à inscrire des informations dans cet équipement et des moyens dont il dispose pour s'y opposer.
    - Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord.
    - Ces dispositions ne sont pas applicables si l'accès ou l'inscription aux informations stockées a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ou est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Mesures de sécurité

- **Les mesures de sécurité « classiques » :**
  - Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées.
  - Il définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme d'assurance. Cette politique devra décrire les objectifs









FICHE N°1

LA PASSATION, LA GESTION ET L'EXECUTION DES CONTRATS D'ASSURANCE (NS 16)

de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

- Les accès aux traitements de données nécessitent une authentification des personnes accédant aux données, au moyen d'un identifiant et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification de même fiabilité.
- Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits…).

● **Les mesures de sécurité pour le site internet :**

- Le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à les rendre incompréhensibles à toute personne non autorisée à y avoir accès.

● **Les mesures de sécurité pour les données de santé :**

- Le responsable de traitement s'engage à respecter les dispositions prévues par le code de bonne conduite annexé à la convention AERAS[12] concernant la collecte et l'utilisation de données relatives à l'état de santé en vue de la souscription ou de l'exécution d'un contrat d'assurance.

Transferts de données hors UE

● **Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'UE et n'assurant pas un niveau de protection adéquat, lorsque :**

- Il existe un niveau suffisant de protection de la vie privée ainsi que des droits et libertés des personnes ou que ces transferts sont juridiquement encadrés (ex : CCT ou BCR),
- Le responsable de traitement a clairement informé les personnes de l'existence d'un transfert de données vers des pays tiers, ou s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert.
- Les transferts sont réalisés dans le cadre de l'exécution des contrats ou de la sauvegarde de la vie humaine pour la mise en œuvre des garanties d'assistance,
- Les transferts sont réalisés lors de la gestion des actions ou contentieux liés à l'activité de l'entreprise (ex : constatation, exercice ou défense de ses droits en justice ou pour les besoins de défense des personnes concernées).

Les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique (niveau de protection adéquat, safe Harbor, CCT, BCR…). Ces transferts d'informations dans le cadre de la passation, la gestion et l'exécution des contrats ayant été expressément prévue par la NS16 aucune autorisation de la CNIL n'est nécessaire, à condition que ces transferts restent impérativement dans le champ de la NS. À défaut, ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert.

(12) Un code de bonne conduite sur l'utilisation des données relatives à l'état de santé a été établi dans le cadre de la convention AERAS (1er février 2011). Il concerne la collecte et l'utilisation des données relatives à l'état de santé en vue de la souscription ou l'exécution d'un contrat d'assurance. Ce code précise les conditions de stricte confidentialité dans lesquelles les données relatives à l'état de santé des assurés doivent être traitées.









FICHE N°2
LA GESTION COMMERCIALE DES CLIENTS ET PROSPECTS POUR LE SECTEUR DES ASSURANCES (NS 56)

LES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI I&L

Finalités poursuivies par le traitement

● **Finalité 1 : les opérations relatives à la gestion des clients concernant :**
- **un programme de fidélité** au sein d'une entité ou plusieurs entités juridiques
- **le suivi de la relation client** tel que la réalisation d'enquêtes de satisfaction, ou le regroupement des contrats pour un même client au sein de l'entreprise ou du groupe auquel appartient l'entreprise.

La norme s'applique expressément au groupe dont fait partie l'organisme déclarant.

● **Finalité 2 : les opérations relatives à la prospection :**
- **la gestion d'opérations techniques de prospection** (ce qui inclut notamment les opérations techniques comme la normalisation, l'enrichissement et la déduplication),
- la sélection de personnes pour réaliser des actions de **fidélisation, de prospection, de sondage, de test produit ou services et de promotion**.
  - Ces opérations ne doivent pas conduire à l'établissement de profils susceptibles de faire apparaître des données sensibles.
  - Il s'agit de cerner les attentes des clients ou le niveau de qualité de services perçus.
  - les programmes de fidélité peuvent être des avantages tarifaires développés par les sociétés d'assurance, des opérations de parrainage….
  - les assureurs peuvent être amenés à tester un nouveau produit d'assurance ou un service associé auprès d'un panel de clients ou de prospects (par exemple, test d'un nouveau produit d'assurance auprès de résidents d'un département, test d'un contrat « chien-chat » auprès d'associations de protection des animaux).
  - Des jeux concours peuvent être également mis à disposition des clients et des prospects (par exemple : permettre de gagner un détecteur de fumée, des objets publicitaires, une invitation à un événement organisé par l'organisme…).
- la réalisation d'**opérations de sollicitations**.

● **Finalité 3 : l'élaboration de statistiques commerciales.**

● **Finalité 4 : la cession, la location ou l'échange des données relatives à l'identification des clients ou prospects pour améliorer le service au client en proposant des produits ou services permettant de réduire la sinistralité ou d'offrir un contrat ou une prestation complémentaire :** Les assureurs sont, à l'image d'autres professionnels, des acteurs économiques qui peuvent céder ou louer leurs fichiers clients ou prospects dans le strict respect des dispositions de la loi I&L, portant notamment sur l'information préalable des personnes (client ou prospect) et leur droit d'opposition. Par exemple, et dans un objectif de prévention, les assureurs peuvent être amenés à céder des fichiers de clients victimes de vol à des partenaires spécialisés en télésurveillance.

● **Finalité 5 : l'organisation de jeux-concours, de loteries ou de toute opération promotionnelle à l'exclusion des jeux d'argent et de hasard en ligne soumis à l'agrément de l'Autorité de régulation des jeux en ligne (ARJEL).**

● **Finalité 6 : la gestion des demandes de droit d'accès, de rectification et d'opposition.** »»



FICHE N°2

LA GESTION COMMERCIALE DES CLIENTS ET PROSPECTS POUR LE SECTEUR DES ASSURANCES (NS 56)

- **Finalité 7 : la gestion des avis des personnes sur des produits, services ou contenus.**

Catégories de données

Une fois les personnes informées de la mise en œuvre du traitement, les données qui les concernent doivent être pertinentes et proportionnées au regard de la finalité.

Les données de santé sont strictement exclues du périmètre de la norme.

- **Les données relatives à l'identification des personnes :**
  - **Les informations classiques** : la civilité, au(x) nom(s), prénoms, adresse, numéro de téléphone (fixe et/ou mobile), numéro de télécopie, adresses de courrier électronique, date de naissance,
  - **Pour l'identification du client ou du prospect** : le code interne de traitement.

Ce code interne de traitement ne peut être le numéro d'inscription au répertoire national d'identification des personnes physiques (numéro de sécurité sociale), ni le numéro de carte bancaire, ni le numéro d'un titre d'identité.

- **La situation familiale, économique, patrimoniale et financière et les habitudes de vie en lien avec la relation commerciale :** il s'agit de la vie maritale, du nombre de personnes composant le foyer, le nombre et l'âge du ou des enfant(s) au foyer, la profession, le domaine d'activité, la présence d'animaux domestiques, les loisirs.
- **Les données relatives aux activités professionnelles et non professionnelles ayant un lien avec la relation commerciale.**
- **Les données relatives au suivi de la relation commerciale :** les demandes de documentation ou de renseignements, les demandes relatives aux produits, services ou abonnements proposés, les montants, la périodicité, les adresses, les données relatives aux produits, les contrats et services, l'origine de la vente (entité ou intermédiaire, vendeur, représentant, partenaire, affilié) ou de la demande, les correspondances avec le client et service client, les échanges et commentaires des clients et prospects, les personne(s) en charge de la relation client, les remises consenties ou avantages client.
- **Les données de localisation et de connexion.**
- **Les données relatives à la sélection de personnes** pour réaliser des actions de fidélisation, de prospection, de sondage, de test produits et services et de promotion.
- **Les données relatives à l'organisation et au traitement des jeux-concours, de loteries et de toute opération promotionnelle** telles que la date de participation, les réponses apportées aux jeux-concours, la photographie ou l'image de la personne, et la nature des lots offerts.
- **Les données relatives aux contributions des personnes** qui déposent des avis sur des produits, services ou contenus, notamment leur pseudonyme.

Durées de conservation

- **Des données relatives à la gestion de clients et de prospects :**
  - Les données des clients sont conservées le temps nécessaire pour la gestion de la relation commerciale.
  - Les données des clients utilisées à des fins de prospection commerciale peuvent être conservées pendant un délai de 3 ans à compter de la fin de la relation commerciale.
  - Les données relatives à un prospect non client peuvent être conservées pendant un délai de 3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect.









FICHE N°2

LA GESTION COMMERCIALE DES CLIENTS ET PROSPECTS POUR LE SECTEUR DES ASSURANCES (NS 56)

Au terme de ce délai, le responsable de traitement peut reprendre contact avec la personne concernée pour lui demander si elle souhaite toujours recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées[1].

- Les données pouvant être utilisées à titre probatoire sont archivées conformément aux dispositions légales.

● **Des pièces d'identité :** pour l'exercice du droit d'accès ou de rectification, les données relatives aux pièces d'identité peuvent être conservées 1 an. En cas d'exercice du droit d'opposition, ces données peuvent être archivées 3 ans[2].

● **Des listes d'opposition à recevoir de la prospection :** les informations permettant de prendre en compte le droit d'opposition de la personne concernée doivent être conservées au minimum 3 ans à compter de l'exercice de ce droit. Ces données ne peuvent en aucun cas être utilisées à d'autres fins que la gestion du droit d'opposition.

● Les informations stockées dans le terminal des utilisateurs (ex : cookies) ou tout autre élément utilisé pour les identifier et les tracer, sont conservés pendant une durée fixée par la doctrine de la CNIL. Les nouvelles visites ne doivent pas prolonger la durée de vie de ces informations. Les données de fréquentation brutes associant un identifiant ne doivent pas être conservées plus de 13 mois selon la recommandation de la CNIL du 5 décembre 2013. Au-delà de ce délai, les données doivent être soit supprimées, soit anonymisées.

Destinataires

● **Peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :**

- Les personnes chargées du service marketing, du service commercial, des services chargés de traiter la relation client, les réclamations, et la prospection, des services administratifs, des services logistiques et informatiques ainsi que leurs responsables hiérarchiques ;
- les services chargés du contrôle (commissaire aux comptes, services chargés des procédures internes du contrôle...) ;
- les sous-traitants dès lors que le contrat signé entre les sous-traitants et le responsable du traitement fait mention des obligations incombant aux sous-traitants en matière de protection de la sécurité et de la confidentialité des données.

● **Peuvent être destinataires des données :**

- Les partenaires et sociétés extérieures (sociétés avec lesquelles l'entreprise entretient des relations commerciales régulières), les entités du groupe de sociétés,
- les auxiliaires de justices, les officiers ministériels et organismes publics habilités à les recevoir, les arbitres, les médiateurs.

Information et droits des personnes

● **La personne doit être informée, préalablement à la mise en œuvre du traitement :** de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.

● **Le recueil du consentement exprès et spécifique de la personne concernée, dans les cas suivants :**

C'est une manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère

(1) Conformément au code de commerce, le code civil et le code de la consommation.
(2) Art 8 et 9 du CPP.





FICHE N°2
LA GESTION COMMERCIALE DES CLIENTS ET PROSPECTS POUR LE SECTEUR DES ASSURANCES (NS 56)

personnel la concernant soient utilisées pour certaines finalités. L'acceptation des conditions générales d'utilisation n'est donc pas une modalité suffisante du recueil du consentement des personnes.

- La prospection réalisée au moyen d'un mode de communication électronique (courrier électronique, SMS ou MMS) hors produits ou services analogues ;
- la prospection réalisée au moyen d'automates d'appel ou de télécopieurs ;
- la mise à disposition ou la cession à des partenaires des adresses électroniques ou des numéros de téléphone utilisés à des fins de prospection par automate d'appel, télécopie ou par envoi de SMS, MMS ;
- la collecte ou la cession des données susceptibles de faire apparaître directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ;
- la collecte de la photographie ou de l'image de la personne.

La participation à un jeu-concours ou une loterie ne peut être conditionnée à la réception de prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique de la part du responsable de traitement ou de ses partenaires.

● **La possibilité de permettre à la personne concernée de s'opposer de manière simple et dénuée d'ambiguïté, dans les cas suivants :**

Dans le cas d'une collecte via un formulaire, le droit d'opposition ou le recueil du consentement préalable doit pouvoir s'exprimer par un moyen simple et spécifique, tel qu'une case à cocher. Les mentions d'information et les modes d'expression de l'opposition ou du recueil du consentement doivent être lisibles, en langage clair et figurer sur les formulaires de collecte.

Lorsque la collecte des données intervient par voie orale, l'intéressé est mis en mesure d'exercer son droit d'opposition ou de donner son consentement avant la collecte de ses données.

- La prospection par voie postale ou téléphonique avec intervention humaine ;
- la prospection réalisée au moyen d'un mode de communication électronique pour un produit ou service analogue ;
- la prospection entre professionnels (sauf en cas d'utilisation d'une adresse générique) lorsque l'objet du message est en rapport avec l'activité du professionnel ;
- la cession d'adresse postale et de numéros de téléphone utilisés à des fins de prospection avec intervention humaine ;
- la cession à des partenaires de données relatives à l'identité (à l'exclusion du code interne de traitement permettant l'identification du client) ainsi que les informations relatives à la situation familiale, économique et financière visées à l'article 3, dès lors que les organismes destinataires s'engagent à ne les exploiter que pour s'adresser directement aux intéressés, pour des finalités exclusivement commerciales.

Après la collecte des données :

● **La personne concernée a le droit de s'opposer, sans frais**, à ce que ses données soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ;

● **Les messages adressés à des fins de prospection directe**, au moyen d'automates



FICHE N°2

LA GESTION COMMERCIALE DES CLIENTS ET PROSPECTS POUR LE SECTEUR DES ASSURANCES (NS 56)

d'appel, télécopieurs et courriers électroniques, doivent mentionner des coordonnées permettant de demander à ne plus recevoir de telles sollicitations.

Le responsable du traitement auprès duquel le droit d'opposition a été exercé informe sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données à caractère personnel qui font l'objet de l'opposition.

L'utilisation d'un site internet

La norme numéro 56 s'applique également dans le cas où le responsable de traitement utilise un site internet pour la gestion des clients et prospects.

- **Les données de connexion (date, heure, adresse internet, protocole de l'ordinateur du visiteur, page consultée) pourront être exploitées à des fins de mesure d'audience et d'assistance technique :** le consentement préalable des personnes n'est pas nécessaire, à condition qu'ils disposent d'une information claire et complète délivrée par l'éditeur du site internet, d'un droit d'opposition, d'un droit d'accès aux données collectées et qu'elles ne soient pas recoupées avec d'autres traitements tels que les fichiers clients dans les conditions prévues par la recommandation du 5 décembre 2013.
- **L'information relative à la finalité et aux droits des personnes :** peut être présente dans les courriers électroniques envoyés, sur la page d'accueil du site, et dans ses conditions générales d'utilisation, etc.
- **L'exercice du droit d'opposition à l'analyse de sa navigation :** l'outil permettant de désactiver la traçabilité mise en œuvre par l'outil d'analyse de fréquentation doit remplir les conditions suivantes :
  - un accès et une installation aisés pour tous les internautes sur l'ensemble des terminaux, des systèmes d'exploitation et des navigateurs internet ;
  - aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.
- **Par ailleurs, tout utilisateur d'un service de communications électroniques doit être informé de manière claire et complète**, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :
  - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
  - des moyens dont il dispose pour s'y opposer.
- **Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition** que la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.
- **Ces dispositions ne sont pas applicables si** l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :
  - soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
  - soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Les mesures de sécurité

- **Le responsable du traitement prend toutes précautions utiles** pour préserver la sécurité des données, et notamment empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.
- **Les accès aux traitements de données doivent nécessiter une authentification** des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification.
- Dans le cas de l'**utilisation d'un site internet**, le responsable de traitement prend



FICHE N°2
LA GESTION COMMERCIALE DES CLIENTS ET PROSPECTS POUR LE SECTEUR DES ASSURANCES (NS 56)

les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à rendre ces données incompréhensibles à toute personne non autorisée.

- **Les pièces d'identité** ne doivent être accessibles qu'à un nombre de personnes restreint et des mesures de sécurité doivent être mises en œuvre afin d'empêcher toute réutilisation détournée de ces données.

Transferts de données hors UE

Seules peuvent être transférées les données pertinentes au regard de la finalité poursuivie par le transfert.

- **La présente norme simplifiée couvre les transferts de données lorsqu'une des conditions suivantes est réunie :**
  - les transferts s'effectuent à destination d'un pays assurant un niveau de protection adéquat ou d'une entreprise américaine ayant adhéré au Safe Harbor ;
  - ils sont encadrés par les clauses contractuelles types (CCT) ou par des règles internes d'entreprise (BCR - Binding Corporate Rules) qui garantissent un niveau de protection suffisant ;
  - ils correspondent à l'une des exceptions de l'article 69 de la loi I&L, limité à des cas de transferts ponctuels et exceptionnels.

Les transferts répétitifs, massifs ou structurels de données personnelles ne sont pas couverts par la présente norme et ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.













FICHE N°3 LA COLLECTE DU NIR ET LA CONSULTATION DU RNIPP (AU 31)

RAPPEL

La Cnil est très attentive aux conditions d'utilisation du NIR qui sont limitées aux finalités prévues dans cette autorisation unique.

LES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI I&L

Finalités poursuivies par le traitement

Les traitements concernés sont uniquement ceux qui interviennent dans le cadre de la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, de réassurance, et d'assistance (périmètre définit par la NS 16).

Finalité 1 : la collecte et le traitement du numéro d'inscription au répertoire (NIR) par les responsables de traitement dans les seuls cas suivants, à l'exclusion de toute utilisation aux fins d'identification des doublons ou des homonymies :

Certains traitements des données à caractère personnel relatifs au numéro NIR peuvent être nécessaires à la passation, à la gestion et à l'exécution des contrats d'assurance. Dès lors, la collecte et le traitement du NIR sont strictement limités aux seuls cas autorisés par la loi.

- pour leurs activités d'assurance maladie[1], maternité, invalidité, retraite supplémentaire[2] ;

Lors de la conclusion d'un contrat de complémentaire santé, l'assureur demande le NIR de l'assuré et des bénéficiaires des garanties pour prendre en charge les frais de maladie et communiquer avec la sécurité sociale dans le cadre du versement conjoint des prestations.*

Lors de la conclusion d'un contrat d'assurance prévoyance couvrant, en plus des risques mentionnés ci-dessus (maladie, maternité, invalidité, retraite) d'autres risques (ex : décès, dépendance…), les organismes d'assurance peuvent, au titre des informations relatives à leurs assurés, détenir le NIR sans le traiter.

(1) L'assurance maladie couvre les frais de santé et d'hospitalisation et également le risque d'incapacité. En outre, il existe une indemnité d'inaptitude versée par la Sécurité sociale qui peut être complétée par les prestations d'organismes d'assurance.
(2) Article R.115-2-2° du code de la sécurité sociale







FICHE N°3
LA COLLECTE DU NIR ET LA CONSULTATION DU RNIPP (AU 31)

- pour leurs activités d'assurance pour les garanties pertes d'exploitation et perte d'emploi uniquement à des fins probatoires;

  Pour la mise en œuvre de ces garanties, les organismes d'assurance sont destinataires de documents (ex: fiches de salaires) sur lesquels figurent le NIR mais qui ne fait pas l'objet d'un traitement.
- pour les relations avec les professionnels, les établissements et les institutions de santé[3] ;

  Les professionnels, institutions ou établissements dispensant à des assurés sociaux ou leurs ayants droit des actes ou prestations pris totalement ou partiellement en charge par l'assurance maladie sont autorisés à utiliser le NIR pour échanger avec les organismes d'assurance. Les organismes d'assurance peuvent donc échanger sur la base du numéro NIR avec les professionnels de santé et les établissements hospitaliers.

  Il en est de même pour les organismes mutualistes et les personnes morales gérées par les institutions de prévoyance.
- pour les déclarations sociales des entreprises souscriptrices de contrats d'assurance[4] ;
- pour l'indemnisation des accidents[5] ;

  Les assureurs ont l'obligation d'informer les caisses d'assurance maladie des lésions causées par leurs assurés à des tiers. Dans le domaine des accidents de la circulation, le code des assurances, oblige les victimes à transmettre, à la demande des assureurs, leur numéro NIR. Le NIR est alors utilisé à des fins de gestion des dossiers d'indemnisation des victimes. Le traitement du NIR permet notamment de donner suite aux recours des tiers payeurs dans le cadre d'un accident avec un responsable.
- pour la gestion des rentes[6] ;

  Le NIR est utilisé pour la gestion des rentes (ex: retraite supplémentaire au régime de base).
- pour l'exécution des dispositions légales, réglementaires et administratives en vigueur.

Finalité 2 : l'accès aux données du Registre National d'Identification des Personnes Physiques (RNIPP) est possible dans les cas suivants:

- pour les traitements mis en œuvre par l'AGIRA qui consiste à:
  - l'existence d'une base de données des personnes dont le décès est connu de l'INSEE,
  - l'interrogation de cette base par les seuls organismes d'assurance vie.
- Les traitements mis en œuvre par les organismes d'assurance ayant pour finalité exclusive la recherche des assurés et bénéficiaires de contrats d'assurance vie qui seraient décédés.

Les modalités de consultation du RNIPP:
- *par voie d'interrogation ponctuelle sur un assuré ou un bénéficiaire,*
- *par voie d'interrogations groupées[7].*

Toute interrogation doit indiquer au minimum les nom(s), prénom(s), date de naissance et sexe de la personne recherchée. Les organismes s'engagent à ne pas utiliser les données de la base AGIRA à d'autres fins que la recherche des assurés bénéficiaires de contrats d'assurance vie qui seraient décédés.

(3) Article R.115-2-3° du code de la sécurité sociale.
(4) Article R-115-2-6° du code de la sécurité sociale.
(5) Articles L.376-1 et L.454-1 du code de la sécurité sociale et plus spécifiquement dans le cadre des accidents de la circulation, en vertu des articles R 211-37 et R 211-38 du code des assurances.
(6) Article 39A de l'annexe III du CGI et L.81 A du livre des procédures fiscales.
(7) Par l'envoi de fichiers portant sur tout ou partie de leurs assurés ou bénéficiaires; ces interrogations groupées pourront porter sur la totalité de la base ou sur les seuls signalements de décès reçus durant la dernière année.



FICHE N°3

LA COLLECTE DU NIR ET LA CONSULTATION DU RNIPP (AU 31)

Catégories de données

- **Le NIR** des personnes parties ou intéressées au contrat : il s'agit par exemple, de l'assuré, du souscripteur, de l'adhérent, du bénéficiaire, du tiers victime ou de l'ayant droit…
- **Les données de la base AGIRA** (et issues du RNIPP) aux fins de recherche des assurés et des bénéficiaires de contrats d'assurance vie qui seraient décédés :
  - nom patronymique, prénoms ;
  - sexe ;
  - date et lieu de naissance ;
  - date et lieu du décès ;
  - numéro d'acte de décès.

Les intermédiaires d'assurance recueillent le NIR lors de la phase de contractualisation (exemple souscription d'un contrat de complémentaire santé). Les partenaires et sous-traitants peuvent intervenir dans le cadre d'un réseau de soins (opticiens, dentistes, audio prothésistes..) et à ce titre collectent le NIR. Les entités d'un même groupe peuvent intervenir dans le cadre d'une mutualisation de moyens ou pour une expertise (ex : médecin conseil « national ») ou lorsque les garanties sont assurées par une entité et vendues par d'autres entités d'un même groupe.

Durées de conservation

- **Le NIR, les données du RNIPP et les données communiquées aux organismes pour la recherche des bénéficiaires d'assurance vie sont conservés pendant la durée nécessaire à l'exécution du contrat.** Elles sont ensuite archivées pour les durées prévues par la loi.
- **Le fichier AGIRA est mis à jour chaque mois** sur la base des éléments transmis par l'INSEE.
- Les données personnelles enregistrées **sont supprimées** lorsqu'il apparaît avec certitude au gestionnaire d'un dossier d'assurance sur la vie qu'elles se rapportent **à un homonyme de l'assuré ou d'un bénéficiaire du contrat.**

Destinataires

- **Peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :**
  - dans le cadre des missions habituelles :
    - les personnels chargés de la passation, la gestion et l'exécution des contrats ;
    - les délégataires de gestion, les intermédiaires d'assurance, les organismes d'assurance chargés dans le cadre d'un contrat de partenariat de gérer les contrats d'assurance du responsable de traitement, y compris dans le cadre d'un réseau de soins ;
    - les sous traitants, les entités du même groupe auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions ;
    - s'il y a lieu les organismes d'assurance des personnes impliquées ;
    - s'il y a lieu, les co-assureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties ;

Il s'agit des co-assureurs et réassureurs qui partagent le risque et à ce titre disposent des données.

    - Les personnes intervenant au contrat ou dans l'instruction des dossiers tels que les avocats, experts, et officiers ministériels, enquêteurs, médecins et autres professionnels de santé et le personnel habilité ;
    - les organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes de sécurité sociale (assurances maladie, maternité, invalidité, décès, assurance retraite supplémentaire) ;
    - les organismes et associations pratiquant la prévention, l'action sociale ou la gestion de réalisations sanitaires et sociales ;









FICHE N°3
LA COLLECTE DU NIR ET LA CONSULTATION DU RNIPP (AU 31)

- **en qualité de personnes intéressées au contrat** : les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats ou les tiers victimes et s'il y a lieu leurs ayants droit et représentants.
- **en qualité de personnes habilitées au titre des tiers autorisés** :
  - Les juridictions concernées, les arbitres, les médiateurs,
  - les autorités de tutelle et de contrôle et tous organismes publics habilités,
  - les services chargés du contrôle (commissaires aux comptes, auditeurs, contrôle interne).

● **Dans le cadre des données relatives aux personnes décédées, les personnes habilitées à recevoir communication de ces données sont :**

- au sein de l'AGIRA, les gestionnaires habilités chargés de l'exploitation des fichiers,
- au sein des organismes d'assurance, des institutions de prévoyance, des mutuelles et de leurs unions :
  - les interrogations sont ponctuelles,
  - effectuées que par un nombre de gestionnaires habilités et limité,
  - disposant de certificats individuels,
  - ayant vérifié la motivation des demandes d'interrogation.

Information des personnes

● **La personne doit être informée, préalablement à la mise en œuvre du traitement :** de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.

● **Par ailleurs, elle dispose d'un droit d'accès, de rectification et d'opposition.**

Mesures de sécurité

La loi « informatique et libertés » impose aux organismes de garantir la sécurité des données.

Cette sécurité est renforcée lors de la collecte du NIR. Le guide « sécurité » élaboré par la CNIL s'adresse à tout responsable de traitement ainsi qu'à toute personne disposant d'un minimum de connaissances informatiques (administrateur système, développeur, responsable de la sécurité des systèmes d'information, utilisateur...) et souhaitant évaluer le niveau de sécurité dont doit bénéficier tout traitement de données à caractère personnel.

● **Les mesures « classiques » :**

- Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données, et notamment empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.
- Il définit une politique de sécurité adaptée aux risques et à la taille de l'organisme. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.
- Les accès aux traitements de données doivent nécessiter une authentification des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification.
- Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits…).

● **Les mesures liées à la base AGIRA :**

- des accès individuels ;
- une authentification mutuelle du système hébergeant le traitement et l'utilisateur[8] ;
- un certificat nominatif ;
- une conservation de l'historique des requêtes effectuées par les organismes ;

(8) *Certificats délivrés par le réseau d'accès aux données de l'assurance et de la messagerie sécurisée (RADAMESS). L'identification des machines connectées au traitement est également faite par des certificats de même nature.*









FICHE N°3
LA COLLECTE DU NIR ET LA CONSULTATION DU RNIPP (AU 31)

- L'AGIRA conserve les interrogations pendant une année ;
- Chiffrement des connexions au traitement et des envois dématérialisés entre l'INSEE et l'AGIRA.

Transferts de données hors UE

Seules peuvent être transférées les données pertinentes au regard de la finalité poursuivie par le transfert.

La présente norme simplifiée couvre les transferts de données lorsqu'une des conditions suivantes est réunie :

- les transferts s'effectuent à destination d'un pays assurant un niveau de protection adéquat ou d'une entreprise américaine ayant adhéré au Safe Harbor ;
- ils sont encadrés par les clauses contractuelles types (CCT) ou par des règles internes d'entreprise (BCR - Binding Corporate Rules) qui garantissent un niveau de protection suffisant ;
- ils correspondent à l'une des exceptions de l'article 69 de la loi I&L, limité à des cas de transferts ponctuels et exceptionnels.

Les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique (niveau de protection adéquat, safe Harbor, CCT, BCR…). Ces transferts d'informations ayant été expressément prévus par l'autorisation unique, aucune autorisation de la CNIL n'est nécessaire, à condition que ces transferts restent impérativement dans le champ de l'AU. À défaut, ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert.









FICHE N°4 LA COLLECTE DES DONNÉES D'INFRACTIONS, DE CONDAMNATIONS OU DES MESURES DE SÛRETÉ (AU 32)

Les organismes d'assurance ainsi que l'AGIRA, effectuent dans le cadre de la passation, de la gestion et de l'exécution des contrats des traitements de données relatifs aux infractions, aux condamnations ou aux mesures de sûreté.

LES TRAITEMENTS DE DONNÉES PERSONNELLES AU REGARD DE LA LOI I&L

Finalités poursuivies par le traitement

- **Finalité 1 : la collecte et le traitement de données relatives aux infractions, condamnations ou mesures de sûreté** prévus par les dispositions légales, réglementaires et administratives en vigueur.
- **Finalité 2 : ces traitements interviennent également dans le cadre des contentieux** liés à l'activité et permettant notamment à l'entreprise d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou la défense des personnes concernées.

Les traitements ne peuvent en aucun cas faire l'objet d'une mutualisation des informations entre les organismes d'assurance à l'exclusion de l'AGIRA.

Les traitements de données relatifs aux infractions, aux condamnations ou aux mesures de sûreté à plusieurs niveaux :

• **soit au moment de la souscription du contrat d'assurance :**

Les données d'infractions et de condamnations font parties des antécédents de l'assuré qui permettent à l'assureur d'évaluer les risques. Ces données peuvent être demandées lors de la souscription de contrats d'assurance de responsabilité civile et en particulier en assurance automobile et responsabilité professionnelle.

En assurance automobile, l'assureur peut décider de majorer la prime en fonction du nombre d'infractions commises par le conducteur. Les infractions sont connues de l'assureur lors de la déclaration du risque. Il pose des questions fermées à la personne qui souhaite souscrire une assurance pour savoir si elle a fait l'objet de condamnations devant une juridiction répressive (ex : conduite sous l'empire d'un état alcoolique ou de stupéfiants, retrait ou suspension de permis de conduire, défaut d'assurance ou de délit de fuite...). Cette information sera également utile à l'assureur en matière de responsabilité professionnelle pour évaluer le risque d'assurance (ex : assurance des mandataires sociaux).

• **soit au cours de son exécution :**

Les données d'infractions peuvent être utilisées à titre de preuve. Par exemple, pour prouver que les conditions de garantie sont remplies et que le risque n'a pas été aggravé, ou encore pour déterminer les responsabilités et procéder à l'indemnisation de la victime.

Exemple :

• Pour le règlement des sinistres et des prestations, il peut s'avérer nécessaire de vérifier les faits qui ouvrent droit à garantie.

• La connaissance des circonstances d'un vol est nécessaire pour vérifier si les conditions de garantie sont réunies. Le dépôt d'une plainte peut être une condition d'indemnisation. Certaines garanties vol peuvent être limitées aux cas d'effraction. Ainsi, conformément aux dispositions prévues dans le contrat, l'assuré devra rapporter la preuve de l'effraction.

• Dans les assurances de responsabilité civile automobile, le procès verbal de police







FICHE N°4

LA COLLECTE DES DONNÉES D'INFRACTIONS, DE CONDAMNATIONS OU DES MESURES DE SÛRETÉ (AU 32)

permet de déterminer les responsabilités de chacun dans l'hypothèse où les circonstances étaient incertaines.

• Par ailleurs, l'assureur a une obligation d'informer la victime qu'elle peut obtenir sur simple demande une copie du procès-verbal. Ainsi, les assureurs de véhicules impliqués dans un accident de la circulation, reçoivent les procès verbaux de police, dans un but d'accélération des procédures d'indemnisation, selon une procédure dénommée « transpv ».

• Au titre de la garantie « recours », l'assureur est amené à exercer le recours de son assuré à l'encontre du Fonds de garantie des assurances obligatoires (FGAO) en cas d'accident et d'absence de responsable identifié ou contre le Fonds de garantie des victimes des actes de terrorisme et d'autres infractions (FGTI) pour les autres infractions. Dans cette hypothèse, il doit recueillir les données relatives aux infractions auprès de son assuré et les transmettre au fond compétent.

• **Pour la gestion des contentieux :**

Dans le cadre des contentieux liés à l'activité d'assurance, ces données peuvent s'avérer nécessaires pour l'entreprise en charge d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou la défense des droits des personnes concernées.

Catégories de données

Il s'agit des données concernant l'assuré, le tiers victime, les ayants droits, les auteurs présumés des infractions ou plus largement toute personne impliquée dans le sinistre (ex : témoins).

Il existe trois grandes catégories de données :

Les données des personnes :
- Les données d'identification : nom et prénom(s), date et lieu de naissance ;
- Les coordonnées postales ;
- Le cas échéant, les données issues des procès verbaux de police ou de gendarmerie, les décisions judiciaires ou administratives et les enquêtes judiciaires.

Les données sur les circonstances de l'infraction :
- Les faits constatés ;
- La présence de témoins, leur identification et leurs témoignages.

Les données postérieures à la constatation de l'infraction :
- Saisine ou absence de saisine ;
- Classement sans suite ;
- Engagement de poursuite ;
- Condamnations ;
- Mesures de sûreté.

Durées de conservation

- La durée de conservation est celle qui est nécessaire à **l'exécution du contrat** ;
- **Les données sont ensuite archivées** conformément aux durées prévues par la loi.

Destinataires

Ils peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :

- **dans le cadre des missions habituelles :**
  - les personnels chargés de la passation, la gestion et l'exécution des contrats ;
  - les délégataires de gestion, les intermédiaires d'assurance, les organismes d'assurance chargés dans le cadre d'un contrat de partenariat de gérer les contrats d'assurance du responsable de traitement ;
  - les prestataires agissant sur ordre du responsable de traitement ;
  - les sous-traitants, ou les entités du groupe d'assurance auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions ;
  - s'il y a lieu les organismes d'assurance des personnes impliquées ou offrant des prestations complémentaires ;
  - s'il y a lieu les co-assureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties ;
  - les personnes intervenant aux contrats tels que les avocats, experts, auxiliaires de justice et officiers ministériels, curateurs, tuteurs, enquêteurs ;
- les organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux.











FICHE N°4

LA COLLECTE DES DONNÉES D'INFRACTIONS, DE CONDAMNATIONS OU DES MESURES DE SÛRETÉ (AU 32)

• **en qualité de personnes intéressées au contrat :**
- les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats ; et s'il y a lieu leurs ayants droit et représentants ;
- s'il y a lieu les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat ;
- s'il y a lieu le responsable, les victimes et leurs mandataires ; les témoins, les tiers intéressés à l'exécution du contrat.

• **en qualité de personnes habilitées au titre des tiers autorisés :**
- s'il y a lieu les juridictions concernées, les arbitres, les médiateurs ;
- les ministères concernés, autorités de tutelle et de contrôle et tous organismes publics habilités à les recevoir ;
- les services chargés du contrôle tels que les commissaires aux comptes et les auditeurs ainsi que les services chargés du contrôle interne.

Information des personnes

• **La personne doit être informée, préalablement** à la mise en œuvre du traitement : de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.

• **Par ailleurs, elle dispose d'un droit d'accès, de rectification et d'opposition**.

Mesures de sécurité

• **Le responsable du traitement prend toutes précautions utiles** pour préserver la sécurité des données, et notamment empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

• Il définit une **politique de sécurité** adaptée aux risques et à la taille de l'organisme. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

• **Les accès aux traitements de données doivent nécessiter une authentification** des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification.

• Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de **traçabilité** (journaux, audits…).

Transferts de données hors UE

Seules peuvent être transférées les données pertinentes au regard de la finalité poursuivie par le transfert.

• La présente norme simplifiée couvre les transferts de données lorsqu'une des conditions suivantes est réunie :
- les transferts s'effectuent à destination d'un pays assurant un niveau de protection adéquat ou d'une entreprise américaine ayant adhéré au Safe Harbor ;
- ils sont encadrés par les clauses contractuelles types (CCT) ou par des règles internes d'entreprise (BCR - Binding Corporate Rules) qui garantissent un niveau de protection suffisant ;
- ils correspondent à l'une des exceptions de l'article 69 de la loi I&L, limité à des cas de transferts ponctuels et exceptionnels.

Les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique (niveau de protection adéquat, safe Harbor, CCT, BCR…). Ces transferts ayant été expressément prévus par l'AU-032, aucune autorisation de la CNIL n'est nécessaire, à condition que ces transferts restent impérativement dans le champ de l'AU. À défaut, ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert.











FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

L'autorisation unique n°39 finalise le pack assurance avec les traitements mis en œuvre dans le cadre de la lutte contre la fraude en assurance. Le travail engagé pour cette autorisation unique a mis en exergue la difficulté d'appréhender à la fois les besoins des assureurs tout en respectant les principes de la loi informatique et libertés et la doctrine de la Commission. Cette complexité s'explique du fait qu'il n'existe pas de définition légale de la fraude à l'assurance. De plus, la fraude est polymorphe. Cette AU se veut la plus large possible et concerne aussi bien la fraude interne et externe.

Périmètre

Pour rappel, le périmètre de la fraude est limité aux seuls organismes d'assurances identifiés dans la norme simplifiée n°16, et s'applique uniquement dans le cadre de la passation, la gestion et l'exécution du contrat d'assurance.

• **La définition** qui a été retenue pour la fraude est la suivante « *tout acte ou omission commis intentionnellement par une ou plusieurs personnes afin d'obtenir un avantage ou un bénéfice de façon illégitime, illicite ou illégal* ».

Ainsi, elle peut revêtir un **caractère pénal** (ex : escroquerie) **ou civil** (ex : faute intentionnelle ou dolosive de l'assuré).

Exemples :

La fraude peut avoir un caractère abusif lorsqu'il s'agit de faire un usage excessif d'un droit, d'un bien ou une pratique au-delà d'une norme de niveau acceptable :

- une sur-tarification des réparations en nature effectuées par un professionnel,

- un alignement des honoraires en fonction des niveaux de garanties maximum des contrats d'assurance,

- une répétition de demandes au-delà de seuils normaux.

• **Classiquement on distingue la fraude interne et la fraude externe en fonction de l'auteur de la fraude :**

Fraude interne	Fraude externe
- le salarié, - l'intermédiaire (agent général, courtier, mandataire…) et ses salariés, - le prestataire (délégation de tout ou partie de la gestion /exécution des contrats), - l'élu, l'administrateur, mandataires sociaux	- les personnes parties ou intéressées au contrat (assurés, bénéficiaires, adhérents, souscripteurs, ayants-droit, tiers victimes…) - les personnes intervenant au contrat (professionnels de santé, prestataires, réparateurs, experts, garagistes, fournisseurs…)









FICHE N°5

LA LUTTE CONTRE LA FRAUDE (AU 39)

Finalités poursuivies par le traitement

● **Finalité 1 : l'analyse et la détection des actes** présentant une anomalie, une incohérence, ou ayant fait l'objet d'un signalement pouvant révéler une fraude à l'assurance.

<u>Exemples d'anomalies ou incohérences :</u>

- La remise de « faux » et « l'usage de faux » lors de la souscription du contrat ou au stade de son exécution (ex : fausse fiche de paie, fausse carte vitale ou faux justificatifs d'identité…),
- Une signature illisible pouvant constituer un indice de fraude qui devra être conforté par d'autres éléments,
- La répétition de plusieurs sinistres pour un même bien ou une même personne,
- plusieurs personnes impliquées pour des mêmes sinistres,
- une incohérence sur les dates indiquées,
- le refus de communication d'une information ou d'un justificatif,
- la modification récurrente d'un RIB ou quasiment concomitante avec la fraude,
- une durée très proche entre la souscription du contrat d'assurance et la réalisation du sinistre,
- des modifications répétées des bénéficiaires d'une clause contractuelle ou quasiment concomitante avec la fraude.

Comment se fait la détection des actes présentant un risque de fraude ?

- dans le cadre de l'activité quotidienne de gestion des commerciaux ou gestionnaires, leur expertise « métier » permet une première analyse humaine d'un fait ou d'un document potentiellement frauduleux (ex : justificatif avec des ratures),
- par le biais d'alertes ou de signalements effectués par des personnes témoins de comportements ou de faits susceptibles de présenter un risque de fraude (collaborateurs internes à l'entreprise, clients, victimes, intermédiaires, enquêteurs, sous-traitant, organismes ou administrations…)
- par un système de requetage automatique élaboré à partir d'une liste de critères préalablement déterminés et pertinents,
- par une analyse manuelle des résultats des requêtes,
- par des contrôles de second niveau (managers, contrôle interne, auditeurs),
- à l'aide de techniques de croisement de données s'appuyant sur des méthodes statistiques et des algorithmes permettant de modéliser des comportements pouvant se révéler frauduleux (scénarios, profils, produits…).

● **Finalité 2 : la gestion des alertes** en cas d'anomalies, d'incohérences ou de signalements,
En cas de fraude avérée, les décisions pouvant en découler sont les suivantes :

Fraude interne	Fraude externe
- contrôles individuels, **- sanctions disciplinaires, procédure de licenciement,** **- résiliation (convention de délégation de gestion, mandat…)** **- engager des procédures contentieuses, judiciaires ….**	**- refuser le versement d'une indemnité ou d'une prestation,** **- refuser d'entrer en relation (ou suspendre l'entrée en relation),** **- engager des procédures amiables, contentieuses…**





FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

- **Finalité 3 : la constitution de listes des personnes** dûment identifiées comme auteurs d'actes pouvant être constitutifs d'une fraude.

Est une « personne présentant un risque de fraude » :
- l'auteur d'un acte présentant une anomalie dont la vérification ne permet pas de lever le doute et qui donne lieu à l'enregistrement dans un fichier. Dès lors, des vérifications doivent être menées afin de lever le doute ou de le confirmer.
- l'auteur d'actes frauduleux ou abusifs. Dès lors, ces personnes peuvent être l'objet de décisions produisant des effets juridiques, et de ce fait être écartées du bénéfice d'un droit ou d'un contrat par exemple.

Les organismes d'assurance sont amenés à constituer de telles listes afin de veiller à respecter la réglementation applicable en matière d'appréciation, de surveillance et de maîtrise des risques et notamment dans le cadre des obligations Solvabilité II.

- **Finalité 4 : la gestion des procédures** amiables, contentieuses, et disciplinaires consécutives à un cas de fraude,

- **Finalité 5 :** l'exécution des **dispositions contractuelles, législatives, réglementaires ou administratives** en vigueur applicables consécutivement à une fraude.

Les traitements de lutte contre la fraude peuvent avoir des conséquences sur les règles légales ou réglementaires à appliquer, notamment fiscales ou sociales, ou peuvent révéler des cas de blanchiment ou de financement du terrorisme.

- L'employeur peut également procéder à des **requêtes individuelles et ponctuelles** dans le cadre de son pouvoir d'enquête interne, sur les données collectées au titre de la gestion administrative du personnel.
- **Les interconnexions** sont possibles dans les conditions suivantes :
  - elles émanent du responsable de traitement ou du groupe auquel il appartient ;
  - elles sont possibles uniquement en matière de :
    - gestion commerciale de clients et de prospects (NS 56) ;
    - passation, gestion et exécution des contrats (NS 16) ;
    - lutte contre le blanchiment et le financement du terrorisme (AU003) ;
    - collecte et traitement des données d'infractions, de condamnations et mesures de sûreté (AU 32) ;
    - gestion des relations contractuelles avec les intermédiaires, les prestataires, les sous-traitants, les délégataires, et les partenaires.

- **Analyse manuelle des alertes détectées automatiquement :**

Les requêtes ou alertes automatiques font l'objet d'une analyse manuelle par le personnel habilité de l'organisme ou du groupe. Il peut également être décidé de procéder à des investigations complémentaires pour confirmer ou non le cas de fraude. Enfin, la personne concernée doit pouvoir présenter ses observations, si une décision produisant des effets juridiques est prise à son égard.

Catégories de données

Les traitements auxquels l'AU fait référence sont ceux préalablement identifiés et encadrés par le biais de normes simplifiées et autorisation unique adoptées par la CNIL. Il s'agit notamment des données dont disposent d'ores et déjà les assureurs dans le cadre de la gestion des contrats d'assurance ainsi que toutes les données nécessaires à l'activité de lutte contre la fraude.




FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

Données relatives à la passation, la gestion et de l'exécution des contrats (NS 16) :
- identification des personnes parties, intéressées ou intervenantes au contrat ;
- situation familiale, économique, patrimoniale et financière ;
- situation professionnelle ;
- appréciation du risque ;
- passation, application du contrat, et gestion des sinistres et des prestations ;
- détermination ou évaluation des préjudices ;
- localisation des personnes ou des biens en relation avec les risques assurés ;
- vie personnelle et habitudes de vie en relation avec les risques assurés ;
- informations relatives à la santé avec le consentement exprès de l'intéressée, sauf s'il ne peut être matériellement ou juridiquement recueilli, ou que l'organisme est soumis à une obligation légale de recueillir ces informations.

Qu'est ce que signifie la localisation des biens ou des personnes ?

Il s'agit des données en lien avec le dossier de fraude (vidéo, photographies et métadonnées). Ne sont pas concernées, les données de géolocalisation des salariés répondant à une finalité autre que la lutte contre la fraude.

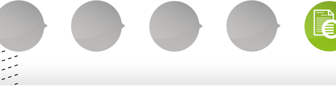
Les données de localisation sont celles qui figurent sur les enregistrements permettant d'horodater et de localiser l'objet de l'enregistrement. Par exemple, une photo envoyée par l'assuré dans le cadre du rapport d'enquête, identifie le lieu du sinistre et sa date. Ainsi, il est possible de constater si la date correspond ou non avec celle de la déclaration du sinistre.

Données relatives à la gestion et au suivi de la relation commerciale (NS 56) :
- identification des personnes ;
- situation familiale, économique, patrimoniale et financière et habitudes de vie en lien avec la relation commerciale ;
- activités professionnelles et non professionnelles ayant un lien avec la relation commerciale ;
- suivi de la relation commerciale ;
- localisation et connexion.

Données relatives aux infractions, condamnations et mesures de sûreté (AU 32) :
- concernant les personnes :
  - les données d'identification : nom et prénom(s), date et lieu de naissance ;
  - les coordonnées postales ;
  - le cas échéant, les données issues des procès verbaux de police ou de gendarmerie, les décisions judiciaires ou administratives et les enquêtes judiciaires.
- concernant les circonstances de l'infraction :
  - les faits constatés ;
  - la présence de témoins, leur identification et leurs témoignages.
- suites données à la constatation de l'infraction :
  - saisine ou absence de saisine ;
  - classement sans suite ;
  - engagement de poursuite ;
  - condamnations ;
  - mesures de sûreté.

À l'occasion de la collecte de données d'infractions, les organismes d'assurance peuvent détecter une fraude. Ou inversement, la découverte d'une fraude peut engendrer la collecte de données d'infraction/condamnation (ex : personne déjà condamnée pour fraude organisée, usurpation d'identité, usage de faux, vol...). De plus, la gestion des actions contentieuses menées suite à des actes frauduleux peut engendrer la collecte de données de condamnations de l'auteur.

Données de journalisation des accès aux traitements (NS 16, NS 56, AU 31 et AU 32).







FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

- **Le NIR** est traité par les organismes uniquement dans les cas suivants :
  - pour les activités d'assurance maladie, maternité, invalidité, retraite supplémentaire, dans le cadre des relations avec les professionnels, les établissements et les institutions de santé, pour les déclarations sociales des entreprises souscriptrices de contrats d'assurance et pour l'indemnisation des accidents,
  - pour la gestion des rentes,
  - enfin, le NIR peut être collecté dans le cadre de leurs activités d'assurance, pour les garanties pertes d'exploitation et perte d'emploi uniquement à des fins probatoires.

Les particularités liées à la collecte et au traitement du NIR

Dans le cadre d'échanges pouvant avoir lieu notamment entre un organisme d'assurance maladie complémentaire et les organismes du régime social obligatoire sur la fraude d'un assuré (ou d'un bénéficiaire ou ayant-droit), le NIR peut faire partie des données transmises :

- soit au titre d'une action en répétition de l'indu menée par l'assurance maladie obligatoire,

- soit au titre d'une action de lutte contre la fraude initiée par l'assurance maladie obligatoire.

- Données collectées au titre de la **gestion administrative du personnel** uniquement dans le cadre de requêtes ponctuelles et individuelles consécutives à la détection d'une fraude.

  Par exemple : vérification de la présence, des absences, la téléphonie, la rémunération, le badgage des salariés…

- Données relatives aux **anomalies, incohérences et signalement** pouvant révéler une fraude.

- Données relatives aux **investigations, à l'instruction** du dossier de fraude et à l'évaluation du **périmètre** de la fraude.

  Exemples de données de gestion d'un dossier de fraude

  *- descriptif des **anomalies, indicateurs, incohérences**, alertes automatiques ou signalement ayant permis de détecter la fraude,*

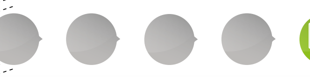
  - **investigations, instruction** *du dossier de fraude et évaluation : descriptif de la fraude, faits, personnes suspectées, témoins, dates, préjudice résultant de la fraude pour l'organisme ou les personnes victimes, rapports d'enquête, expertises, durée, montant, nombre de personnes impliquées, décisions prises par l'organisme,*

  *- **données issues des bases de données internes** (bases relation client, gestion des contrats, gestion du personnel ou des intermédiaires, …) ou de **fichiers externes** (Agira, messagerie Alfa, Argos…) ou encore de **bases externes et registres** qui sont destinés exclusivement à l'information du public et sont ouverts à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime.*

  Il s'agit par exemple de vérifier que les informations données par la personne concernée et celles détenues par les organismes administratifs ou professionnels sont concordantes avec celles de l'assureur (antécédents déclarés, par exemple le relevé d'information en matière de sinistres auto retrace les sinistres sur une période de 5 ans, validité carte grise, inscription RCS, véhicule déclaré volé chez un autre assureur…).

- **Données d'identification des personnes intervenant dans la détection et la gestion de la fraude.**

  Exemple : les enquêteurs et les personnes impliquées dans l'enquête, dont l'usage de pseudonymes, ou identités fictives destiné à protéger ces personnes,







FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

Durées de conservation

● **Étape n°1 / qualification de l'alerte** : à compter de l'émission de l'alerte, les organismes d'assurance disposent d'un délai de 6 mois pour qualifier les alertes. Toute alerte « non pertinente » ou n'ayant reçu aucune qualification à l'issue du délai de 6 mois, doit être supprimée immédiatement.

● **Étape n°2 / alerte qualifiée** : lorsque l'alerte est « pertinente » les données sont conservées pour une durée maximale de 5 ans à compter de la clôture du dossier de fraude. En cas de procédure judicaire, elles sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées.

S'agissant de la possibilité d'inscription dans le fichier des personnes présentant un risque de fraude, les données sont conservées pendant une durée de 5 ans à compter de la date d'inscription.

Destinataires

Peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :

● **Les destinataires « classiques » :**

Fraude interne	Fraude externe et interne
- personnes habilitées DRH (requêtes ponctuelles et individuelles) ; - conseil de discipline saisi en cas de fraude ; - les représentants du personnel dans le cadre de l'accompagnement d'un salarié mis en cause pour fraude.	- les personnels en relation avec la clientèle et les gestionnaires de contrats et de sinistres ; - les autres entités d'un même groupe dès lors qu'elles sont concernées par la fraude ou interviennent dans la gestion des dossiers ou de maîtrise du risque de fraude ; - les personnels habilités en charge de la lutte contre la fraude, de la lutte antiblanchiment et du contrôle interne ; - les inspecteurs, enquêteurs, experts, et auditeurs ; - le personnel habilité de la direction générale, la direction juridique ou du service du contentieux pour la gestion des contentieux ; - le personnel habilité des sous-traitants.

● **Les destinataires « directement concernés par une fraude » :**

- les autres organismes d'assurance ou intermédiaires intervenant dans le cadre de dossier présentant une fraude,
- les organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux ;
- les organismes professionnels intervenant dans le cadre de dossiers présentant une fraude ;
- les auxiliaires de justice et officiers ministériels ;
- l'autorité judiciaire, médiateur, arbitre saisis d'un litige ;
- les organismes tiers autorisés par une disposition légale à obtenir la communication de données à caractère personnel relatives à des précontentieux, contentieux ou condamnations ;
- s'il y a lieu les victimes de fraudes ou leurs représentants.

La communication de ces données ne peut en aucun cas donner lieu à la création d'un fichier concernant les données relatives aux fraudes et mutualisé entre les destinataires.









FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

Information des personnes

Il existe 2 niveaux d'information :

- **Premier niveau** : information générale des personnes concernées sur le dispositif de lutte contre la fraude pouvant conduire à l'inscription sur la liste des personnes à risque.

Il existe des modalités d'information distinctes en fonction des personnes visées :

Fraude interne	Fraude externe
- les salariés de l'organisme d'assurance sont informés individuellement dans le règlement intérieur ou dans tout autre support de communication échangé lors de l'exécution du contrat, **- les prestataires, les agents généraux, les mandataires, les intermédiaires, les administrateurs, les mandataires sociaux ou les élus des organismes sont informés dans les documents contractuels ou tout autre support de communication adressés par l'organisme d'assurance.**	**- les assurés sont informés de l'existence du traitement dans les documents communiqués au moment de la souscription du contrat, ou de tout autre support de communication échangé lors de l'exécution du contrat.**

- **Second niveau** : Le responsable de traitement informe systématiquement lors de la contractualisation de la mise en œuvre d'un dispositif de lutte contre la fraude susceptible de conduire à l'inscription sur une liste de personnes présentant un risque de fraude. Les conséquences en cas de fraude sont régies par les dispositions contractuelles.

En cas de détection d'une anomalie, d'une incohérence ou d'un signalement susceptible de relever d'une fraude, le responsable de traitement a la possibilité d'inscrire une personne sur une « liste de personnes présentant un risque de fraude ». La personne concernée, susceptible d'être inscrite sur cette liste peut être un assuré, un prestataire, un professionnel de santé etc. (Il s'agit des personnes concernées par la mise en œuvre du traitement de lutte contre la fraude interne et externe).

Au cours de la période d'investigation, la personne concernée peut être contactée, selon le type de fraude suspectée (assuré, partenaire, salarié…), pour apporter des explications complémentaires.

Au terme des investigations, et en cas de décision prise produisant des effets juridiques (refus de prise charge, avertissement au salarié, rupture de contrat), une information écrite et individuelle est adressée précisant les mesures prises par l'assureur (conséquences de l'application du contrat concerné) et lui donnant la possibilité de présenter ses observations.

Mesures de sécurité

- **Le responsable du traitement prend toutes précautions utiles** pour préserver la sécurité des données, et notamment empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.
- Il définit une **politique de sécurité** adaptée aux risques et à la taille de l'organisme. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.
- **Les accès aux traitements de données doivent nécessiter une authentification** des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification.











FICHE N°5
LA LUTTE CONTRE LA FRAUDE (AU 39)

- Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de **traçabilité** (journaux, audits…). Il en va de même pour les interventions de maintenance qui doivent faire l'objet d'une traçabilité. Par ailleurs, le matériel remisé devra être nettoyé de toute donnée à caractère personnel.
- S'il existe **un site internet**, le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées.
- Le responsable de traitement devra aussi **s'assurer que ses sous-traitants présentent des garanties** en matière de sécurité des données.
- **S'agissant des données de santé**, le responsable de traitement s'engage à respecter le code de bonne conduite annexé à la convention AERAS concernant la collecte et l'utilisation de données relatives à l'état de santé en vue de la souscription ou de l'exécution d'un contrat d'assurance.

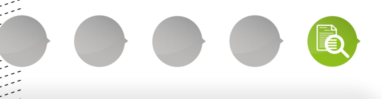
Transferts de données hors UE

Seules peuvent être transférées les données pertinentes au regard de la finalité poursuivie par le transfert.

- **La présente autorisation unique couvre les transferts de données lorsqu'une des conditions suivantes est réunie :**
  - les transferts s'effectuent à destination d'un pays assurant un niveau de protection adéquat ou d'une entreprise américaine ayant adhéré au Safe Harbor ;
  - ils sont encadrés par les clauses contractuelles types (CCT) ou par des règles internes d'entreprise (BCR - Binding Corporate Rules) qui garantissent un niveau de protection suffisant ;
  - ils correspondent à l'une des exceptions de l'article 69 de la loi I&L, limité à des cas de transferts ponctuels et exceptionnels.

Les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique (niveau de protection adéquat, safe Harbor, CCT, BCR…) Ces transferts d'informations dans le cadre de l'activité de lutte contre la fraude ayant été expressément prévus par l'AU-039, aucune autorisation de la CNIL n'est nécessaire, à condition que ces transferts restent impérativement dans le champ de l'AU. À défaut, ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert.





PRÉCISIONS SUR LE SORT DES FORMALITÉS PRÉALABLES DÉJÀ ACCOMPLIES AUPRÈS DE LA CNIL

Un organisme d'assurance ayant procédé à un engagement de conformité à la NS 16 dans son ancienne rédaction, et qui ne modifie pas son traitement compte tenu de la nouvelle norme, n'a pas à accomplir une nouvelle formalité.

L'organisme d'assurance qui ne modifie pas son traitement déclaré en référence à l'AU 18, n'a pas besoin de faire un nouvel engagement de conformité à l'AU 31 (qui intègre l'AU 18) à moins que cet organisme ne collecte le NIR.

Enfin, tout projet de traitement dont les finalités ou les catégories de données ou de destinataires excéderaient le cadre défini par les autorisations uniques et qui ne respecterait pas les exigences qui y sont définies devra faire l'objet d'une demande d'autorisation spécifique présentant et expliquant les différences entre le traitement envisagé et l'autorisation unique concernée.

CONCLUSION GÉNÉRALE SUR LE PACK ASSURANCE

Le pack de conformité assurance permet donc de recenser et d'encadrer l'ensemble des traitements mis en œuvre par les acteurs (organismes d'assurance, intermédiaires, sociétés d'assistance) pour toutes les branches d'assurance y compris l'assistance. Ce pack concerne également les « Groupes » auxquels appartiennent les responsables de traitement. Cette démarche s'inscrit dans une logique de sécurisation juridique apportée aux professionnels et une meilleure prise en compte de la réalité de leurs activités, qui caractérise la nouvelle méthode de travail de la Cnil pour accompagner les responsables de traitement dans leur mise en conformité avec la loi informatique et libertés, non seulement en matière de formalités mais dans la substance des traitements de données personnelles concernés. Les échanges ont permis de dégager un cadre réglementaire lisible et opérationnel faisant également référence à des garanties prévues par d'autres instruments juridiques. Par exemple, le code de bonne conduite annexé à la convention AERAS qui vise les conditions de collecte et d'utilisation des données de santé.

Par ailleurs, les deux normes simplifiées et les trois autorisations uniques, complétées par des fiches pratiques représentent une simplification des formalités telle qu'elle est souhaitée par la Commission et attendue par les professionnels.

Vers la création d'un Club conformité

Afin de tirer parti de l'espace privilégié d'échanges qui s'est créé entre la Cnil et les professionnels pour élaborer le pack de conformité, le groupe de travail initialement constitué va continuer à se réunir périodiquement, sous la forme d'un « club conformité ». Il s'agira de ne pas perdre le bénéfice apporté par cette zone de confiance pour débattre des besoins et questionnements sur l'application de la loi, évaluer dans le temps la robustesse des outils de régulation des données ayant été élaborés, les mettre à jour en fonction tant de l'évolution des métiers que de la législation, enfin, créer un effet d'entraînement vertueux dans la diffusion de la conformité informatique et libertés grâce à l'action démultiplicatrice des réseaux professionnels impliqués.